2766

Docket Number: 0225-4188

#8/B

BH 5-18-01





**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of
Argen K. LENSTRA, and
Eric R. VERHEUL

Serial No: 09/498,716

Filed: February 7, 2000

For: EFFICIENT AND COMPACT SUBGROUP TRACE REPRESENTATION ("XTR")

Group Art Unit: 2766

Examiner: Unassigned

## SUPPLEMENTAL PRELIMINARY AMENDMENT

Commissioner of Patents
Washington, D.C. 20231

Dear Sir,

Prior to a review on the merits, please amend the above-identified application in the following manner.

## IN THE SPECIFICATION

Appendix 1 includes a marked-up version of the paragraphs and sections in the specification that this Amendment replaces.

**REPLACE the paragraph on page 3, lines 13-29 of the Substitute Specification with the following:**

B1

The method of the invention determines a public key having a reduced length and a number $p$, using GF($p$) or GF($p^2$) arithmetic to achieve GF($p^6$) security, without explicitly constructing GF($p^6$). The method includes the step of selecting a number $p$ and a prime number $q$ that is a divisor of $p^2 - p + 1$. Then the method selects an element $g$ of order $q$ in GF($p^6$), where $g$ and its conjugates can be represented by $B$, where $F_g(X) = X - BX^2 + B^p X - 1$ and the